

POLICY 1.00 FIREWALL CONFIGURATION & MANAGEMENT

The Office for Information Resources (OIR) is responsible for, and has the authority to establish and control firewall configuration and management.

PURPOSE:

To ensure consistent, compatible firewall products and related access controls are implemented both within the State of Tennessee networks and between the State of Tennessee's networked egresses to the Internet or any other computer networks.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994

OBJECTIVES:

1. Limit inbound and outbound services among internal computer networks and between the Internet to only those services required for authorized State business functions.
2. Ensure the reliability and integrity of State information systems data.
3. Safeguard information assets from exposure to external threats from disruption, interference, unauthorized access, misuse, theft, denial of service, or other potentially destructive activity.
4. Define information systems management and user responsibilities and accountabilities in the protection of information technology resources.
5. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.

SCOPE:

The scope of this policy includes all connections among internal networks and between any publicly accessible computer network, and includes all other connections between the State of Tennessee computer systems networks and external public or private organizations.

IMPLEMENTATION:

Office for Information Resources (OIR)

1. Ensure firewall management remains strictly controlled.
2. Ensure access control to the firewall and/or operating system to prevent unauthorized access should a firewall platform component be compromised or cease to function.

3. Ensure consistent application of approved rules and configurations on all firewalls.
4. Establish standards and implement secure firewall operating system configurations.
5. Ensure timely implementation of software patches, upgrades and releases.
6. Provide hardware and software maintenance, backup and recovery services to ensure reliable and available services.
7. Ensure only essential services are deployed on each firewall.
8. Restrict access to firewall information such as network addresses, configurations, and attached networks or systems.
9. Provide centralized monitoring and management of all firewalls deployed on the State network.

Agency

1. Identify agency processes and services requiring firewall technology.
2. Implement agency processes and procedures in support of State firewall policy and procedures.
3. Confirm agency firewall rulesets through periodic reviews.
4. Refrain from implementing agency procedures, processes or practices that would expose networked information resources to unnecessary or unauthorized risks.

Individual Users/Clients

1. Adhere to statewide and agency policies, standards, procedures and guidelines with respect to networks, systems, applications and data security.
2. Refrain from behaviors that would expose networked information technology resources to unnecessary or unauthorized risks.